	Georgia Technology Authority	
Title:	**Implementing Cryptographic Controls**	
PSG Number:	SS-08-040.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 3
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes the minimum requirements for the use of cryptographic controls.	

PURPOSE

Cryptography is a discipline that embodies principles, means and methods for providing several security services: confidentiality, data integrity, authentication and non-repudiation.

Where the confidentiality, authenticity, or integrity of information is critical, the use of cryptographic controls may be warranted.

This standard establishes the minimum requirements for the use of cryptographic controls.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARDS

Agencies shall select cryptographic technology based on the security objectives, applicable policies, laws and regulations and performance requirements.

When selecting cryptographic technologies, agencies shall use only those algorithms, keys, modules and implementations that are FIPS-compliant and/or NIST-recommended. The use of other encryption algorithms is NOT allowed for any purpose.

Cryptographic modules used for State of Georgia information systems shall comply with a security level rating of 2 or higher (defined in FIPS 140-2 and its successors) as required to meet security requirements.

Agencies shall implement end-to-end cryptographic security controls for, but not limited to, the following:

- for identity and authentication credentials in storage or transit
- when non-repudiation is required
- to store cryptographic algorithm and key information
- for secure wireless communications
- for ANY highly sensitive data or communications where the risk of compromise or exposure is higher than acceptable and compensating controls are insufficient

Security officers and/or cryptographic officers shall:

- be properly trained to ensure the continued secure operations and maintenance of the cryptographic components and proper destruction or archive of keys when a system is decommissioned.
- be notified and participate in any process where cryptographic systems are modified and ensure all changes are in accordance with change management policies and procedures.
- be notified when a cryptographic system, encrypted data or transmission is believed to be exposed or compromised.

SUPPLEMENTAL EXCEPTION

Encrypted data shall be decrypted prior to being transferred to the Georgia Archives for long term storage. The Georgia Archives shall assume responsibility for providing appropriate control measures to maintain the confidentiality, integrity, availability and non-repudiation of the information in their charge.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Use of Cryptography (Policy)

REFERENCES

- NIST SP 800-12 (chapter 19) Introduction to Computer Security NIST Handbook
- NIST SP 800-21 Guideline for Implementing Cryptography in the Federal Government
- FIPS 140-2 Security Requirements for Cryptographic Modules
- NIST 800-57 Recommendation for Key Management
- NIST 800-56 Recommendations for Pair-Wise Key Establishment Schemes
- NIST Cryptographic Key Tool Kit http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html

TERMS and DEFINITIONS

Cryptography - A branch of applied mathematics (algorithms) concerned with

encrypting and decrypting data such that the sender's identity (authentication and non-repudiation), data confidentiality, integrity or origin can be assured.

- **Encryption** - The process of converting ordinary information (plain text) into unintelligible character strings (i.e., *ciphertext*).
- **Decryption** - The reverse, moving from unintelligible ciphertext to plaintext.
- A **cipher** (or *cypher*) - A pair of algorithms which perform this encryption and the reversing decryption.
- **Key** (or cryptographic key) - A parameter used in conjunction with a cryptographic algorithm that an entity with knowledge of the key can reproduce or reverse the operation (encrypt or decrypt) while an entity without knowledge of the key cannot.

Non-Repudiation - A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party.

Authentication - A process that establishes origin of information or determines an entity's identity.

Advanced Authentication (also referred to as strong authentication) - Uses techniques that require multi-factor identity credentials to confirm a user's identity and/or authority to access information resources.

Identity/authentication credentials are information known only to a user and recognized by the system such as passwords, private keys, symmetric keys, tokens, biometric data or digital signature algorithm used to positively identify that user and allow access to system resources.

Note: The PSG number was changed from S-08-040.01 on September 1, 2008